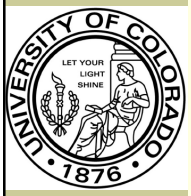


Security Issues Related to Cognitive Radios and Dynamic Spectrum Access

Timothy X Brown
Interdisciplinary Telecommunications Program
Dept. of Electrical, Computer, and Energy Engineering
University of Colorado, Boulder

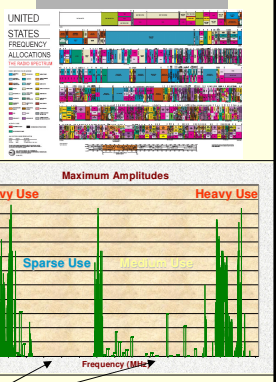
11th Annual International Symposium on Advanced Radio Technologies
Boulder, CO July 27 2010

CR/DSA Security

- Why are CR/DSA special?
- 50 ways to deny your service.
- How to analyze and harden CR systems.

Review

- Spectrum is important to UAS
- The spectrum is fully allocated
- Most spectrum is unused
- Cognitive Radio:
  - Avoid Licensed users
  - Communicate in “white spaces”



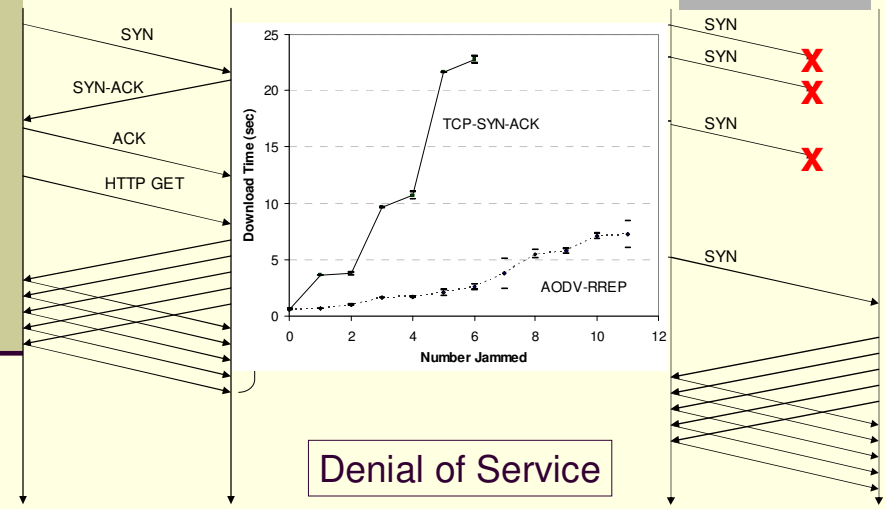
The Big Question

Can CR/DSA be made secure?

Confidentiality
Integrity → Similar to other wireless devices

Availability → Vulnerable to Denial of Service

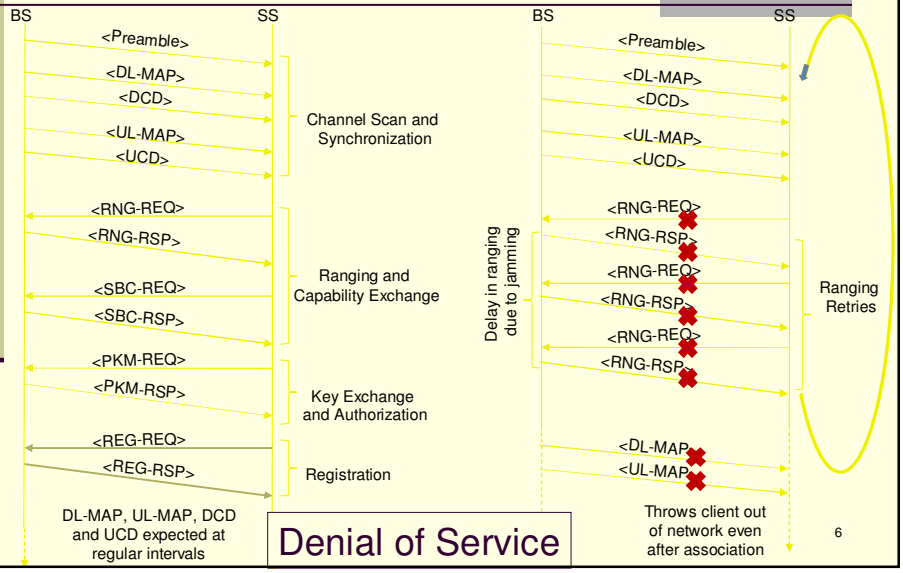
TCP Denial of Service



Denial of Service

Brown, James, Sethi, "Jamming and Sensing of Encrypted Wireless Ad Hoc Networks," in *MobiHoc*, 2006

802.16 Network Entry and Initialization Denial of Service



Denial of Service

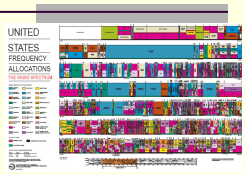
DSA/CR being pushed for

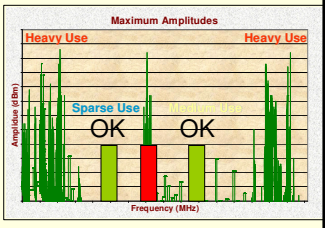
- Commercial
- Public Safety
- Military

Will not tolerate Denial of Service

Need to be careful with spectrum

- The spectrum is fully allocated
- Primary users fear Harmful Interference
- "Mistakes" will bring down regulatory hammer.

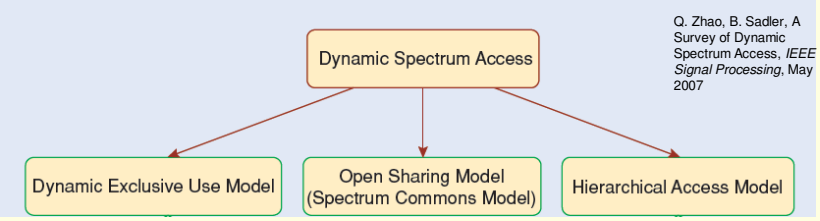




Whoops!

Review

Many DSA concepts



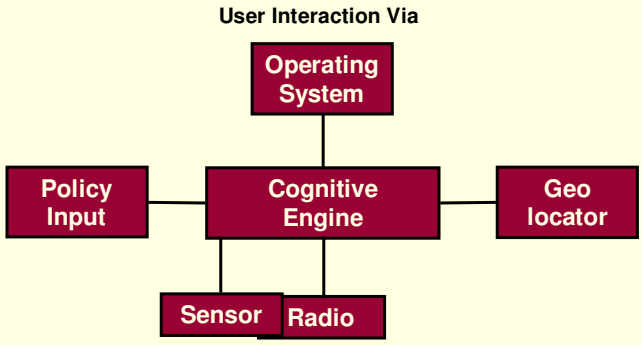
Q. Zhao, B. Sadler, A Survey of Dynamic Spectrum Access, *IEEE Signal Processing*, May 2007

- Fast buy and sell
- Short-term Rental

- Unlicensed
- Access etiquettes

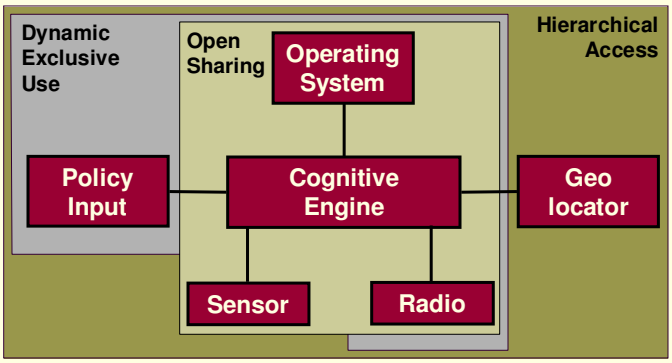
- Find whitespaces
- Avoid harming primary

Cognitive vs. Traditional Radios



A CR does more than a traditional radio

Cognitive vs. Traditional Radios



Not all functions used in all cognitive radios
What are the most vulnerable?

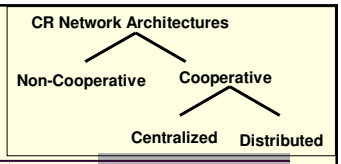
Why are CR/DSA different?

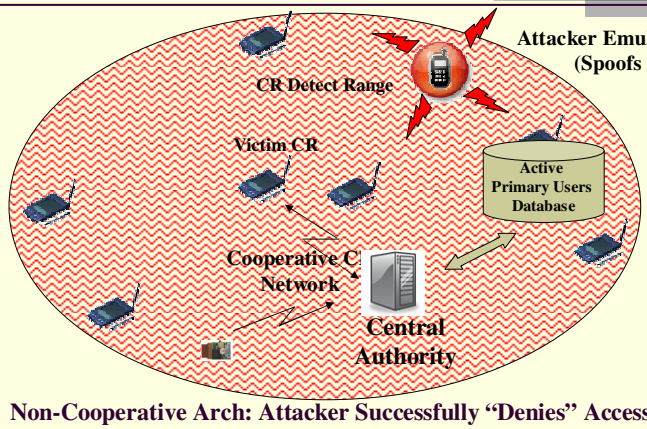
- More functions:
  - more functions = more vulnerabilities
- Two DoS attacks:
  - Directly: degrade one or more radios
  - Indirectly: induce harmful interference
- Wide range of architectures
  - What are best choices?

CR/DSA Security

- Why are CR/DSA special?
- 50 ways to deny your service.
- How to analyze and harden CR systems.

Example: CR-specific DoS Attack



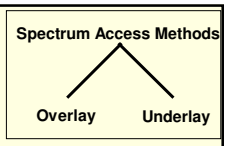


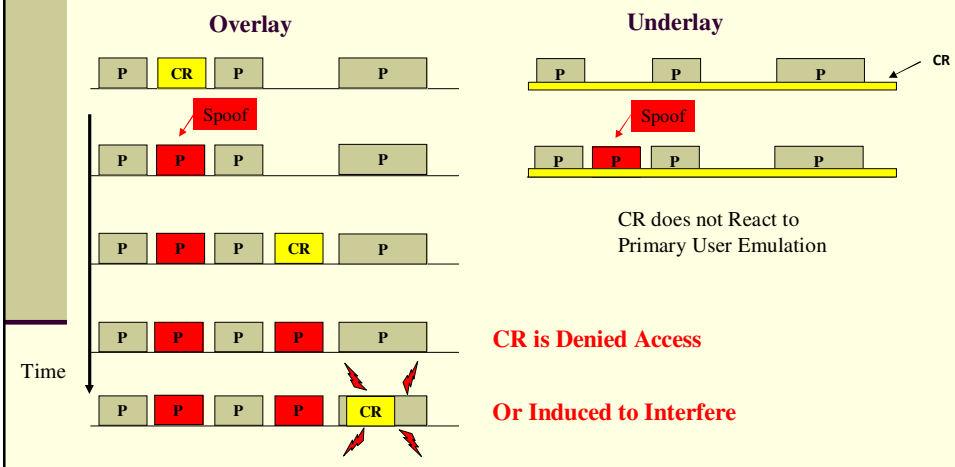
Non-Cooperative Arch: Attacker Successfully "Denies" Access

Distributed Cooperative Arch: Collated measurements make the attack less effective.
Centralized Cooperative Arch: Ineffective due to collated measurements in DB

Vulnerability Depends on Architecture

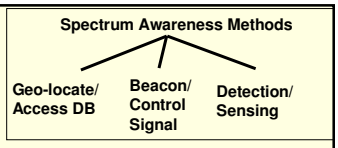
Example CR-specific DoS Attack





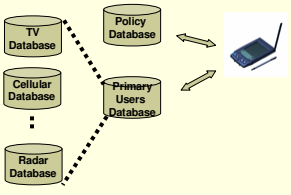
Vulnerability Depends on Spectrum Access Methods

Spectrum Awareness



Prone to Location/DB Spoof, Jam, Replay

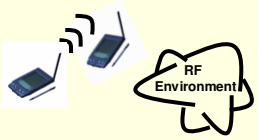
Geo-locate/ Access DB



Beacon/ Control Signal

Prone to Beacon/Control Signal Spoof, Jam, Relay

Detection/ Sensing

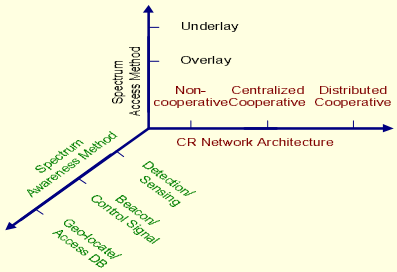


Prone to Sensing Spoof, Jam, Replay

Vulnerability Depends on Spectrum Awareness Methods

Many Attacks and Many Cofigurations

Attacker …
injects policies that prevent CR communication on specific primary channels.
injects policies that deny CR communication on all primary channels.
injects policies that allow CR communication on specific primary channels.
injects policies that induce CR communication on all primary channels.
emulates primary user on all primary channels.
emulates primary user on specific primary channels.
masks primary user on specific occupied primary channels.
blocks location information
jams at spectrum handoff.
bloc
bloc
indu
induces receiver errors on multiple licensed channels.



Analysis of Multiple Attacks against Multi-Dimensional CR Configurations

CR/DSA Security

- Why are CR/DSA special?
- 50 ways to deny your service.
- How to analyze and harden CR systems.

Analysis Approach

- Combines
  - likelihood/impact risk assessment (Barbeau/ETSI TS 102 165-1 V4.1.1)
  - aviation risk analysis techniques (Hammer)
- Two Analyses
  - Open: e.g. no encryption
  - Hardened

Qualitative ranking

Organizes complex interactions

Attack Analysis: Risk Assessment (1/3)

1. Attack Likelihood

Technical Problems to Attacker	Likelihood Case	Rank
Insolvable	**Impossible**	**0**
Strong	**Low**	**1**
Solvable	**Medium**	**2**
None	**High**	**3**

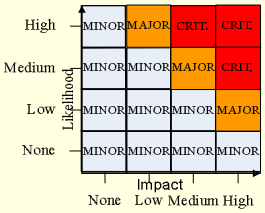
Attack Analysis: Risk Assessment (2/3)

2. Attack Impact

Rationale: Impact on Victim		Impact Case	Rank
Denial Attacks	Induce Attacks		
None	**None**	**None**	**0**
Perceptible but insignificant degradation in CR communication.	**Perceptible but infrequent interference to active primary users**	**Low**	**1**
Significant degradation but still operational CR communication.	**Perceptible frequent interference to active primary users**	**Medium**	**2**
Non-operational CR communication	**Continuous interference to active primary users**	**High**	**3**

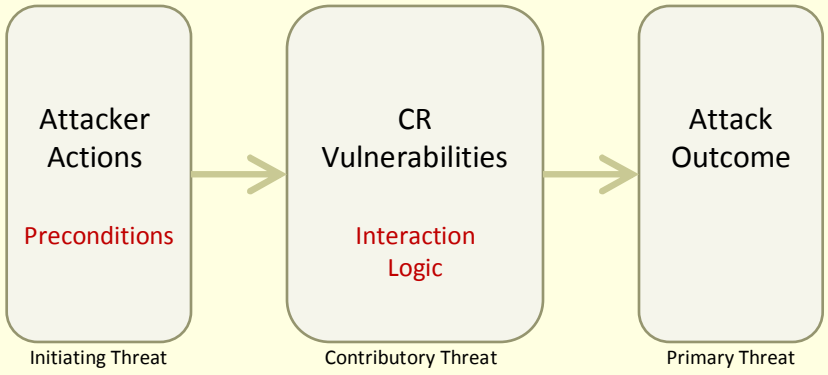
Attack Analysis: Risk Assessment (3/3)

3. Risk Level = *f*(Likelihood, Impact)



Risk Case	Risk Mitigation Action
Minor	**No Countermeasures Required**
Major	**Threat cannot be Ignored**
Critical	**Mandates High Priority Handling**

Attack Analysis: Risk Analysis using Hammer Model Framework (1/3)

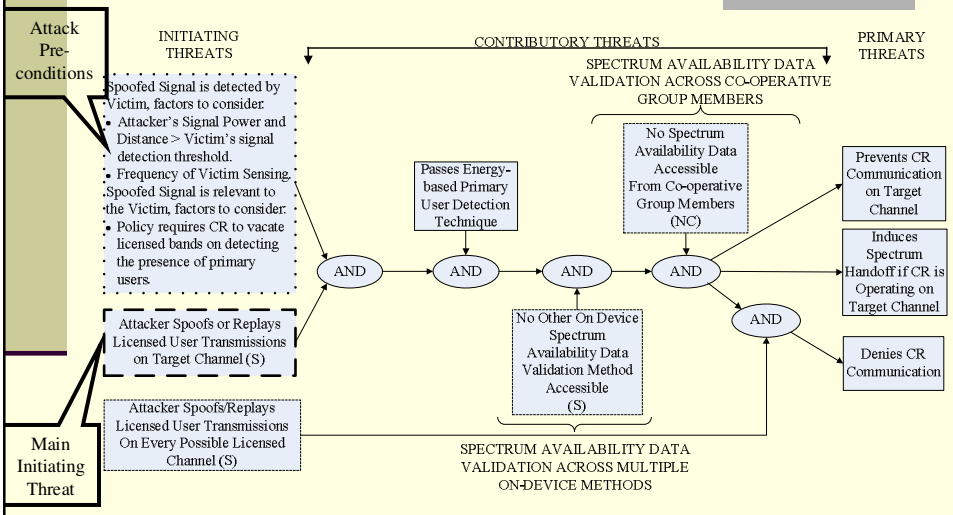


- Organizes complex interactions
- Based on FAA System Safety Hazard Analysis

Attack Analysis: Risk Analysis using Hammer Model Framework (2/3)

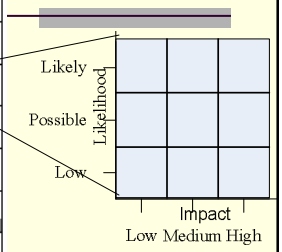
- Modeling tool to represent an attack scenario into a sequence of initiating and contributory threats that result in one of more primary threats.
- Primarily Used for Qualitative Scenario based Attack Analysis.

Example: Primary User Emulation Attack in Non-Cooperative Architecture (3/3)



Open System Attack Analysis Summary

Attacker …	Bea-con	Geo+ DB	Detect Sense
injects policies that prevent CR communication on specific primary channels.	■	■	
injects policies that deny CR communication on all primary channels.	■	■	
injects policies that allow CR communication on specific primary channels.	■	■	
injects policies that induce CR communication on all primary channels.	■	■	
emulates primary user on all primary channels.			■
emulates primary user on specific primary channels.			■
masks primary user on specific occupied primary channels.			■
blocks location information		■	
jams at spectrum handoff.	■	■	■
blocks access to networked sensor information.			■
blocks access to policies.	■	■	
induces receiver errors on specific licensed channel			■
induces receiver errors on multiple licensed channels.			■



Assumes open system with no encryption on any link

CR/DSA Security

- Why are CR/DSA special?
- 50 ways to deny your service.
- How to analyze and harden CR systems.

System Hardening

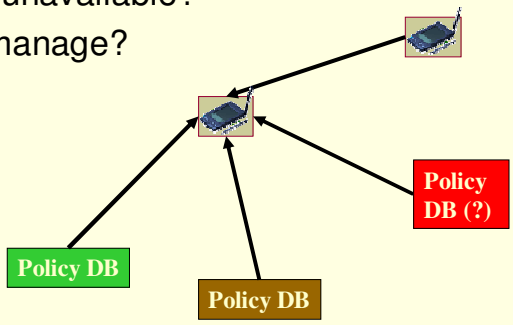
Can we mitigate:

- Primary User Emulation Attack
- Policy Spoofing
- Beacon Replay Attack
- Location Denial of Service
- …

Example:

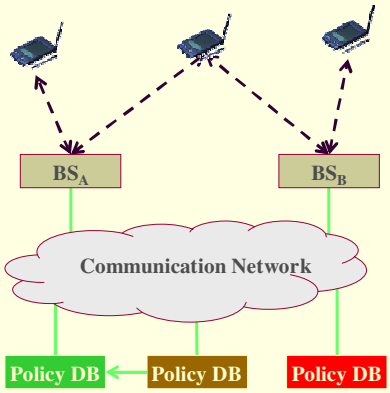
How to Get Policies

- Simplest mechanism: Someone tells you
  - Who do you trust?
  - What if DB is unavailable?
  - How do you manage?

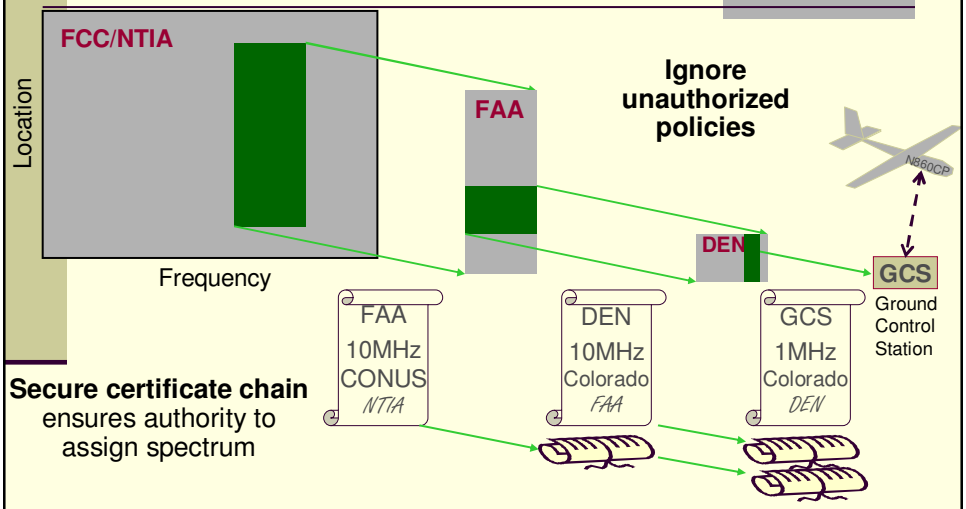


Policy Communication Model

- Example: Centralized Model



Hierarchical Policy Authorization



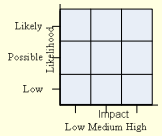
Secure certificate chain ensures authority to assign spectrum

How can we harden the DSA/CR?

- Digital Signatures (false messages)
- Encrypted control channels (coordinated attacks)
- Spread spectrum control channels (jamming)
- Trust/reputation (malicious messages/users)
- Cooperative analysis (primary user emulation)
- Cooperative policing (unauthorized spectrum access)
- Multi-mode geolocation (GPS jamming)
- Multi time-scale policies (policy/beacon jamming)

Hardened System Attack Analysis Summary

Attacker …	Beacon	Geo-DB	Detect Sense
injects policies that prevent CR communication on specific primary channels.	■	■	
injects policies that deny CR communication on all primary channels.	■	■	
injects policies that allow CR communication on specific primary channels.	■	■	
injects policies that induce CR communication on all primary channels.	■	■	
emulates primary user on all primary channels.			■
emulates primary user on specific primary channels.			■
masks primary user on specific occupied primary channels.			■
blocks location information		■	
jams at spectrum handoff.	■	■	■
blocks access to networked sensor information.			■
blocks access to policies.	■	■	
induces receiver errors on specific licensed channel			■
induces receiver errors on multiple licensed channels.			■



Assumes strongest mitigation technique identified

Risk Assessment Results

CR Configuration used in 802.22

	Overlay			Underlay		
	Beacon	Geo-locate Database	Detection Sensing	Beacon	Geo-locate Database	Detection Sensing
Non-Cooperative	1, 2	0, 3	0, 2	0, 2	0, 1	0, 2
Centralized Cooperative	0, 3	0, 3	0, 3	0, 1	0, 1	0, 2
Distributed Cooperative	0, 3	0, 3	0, 2	0, 1	0, 1	0, 2

(*Critical, Major*)

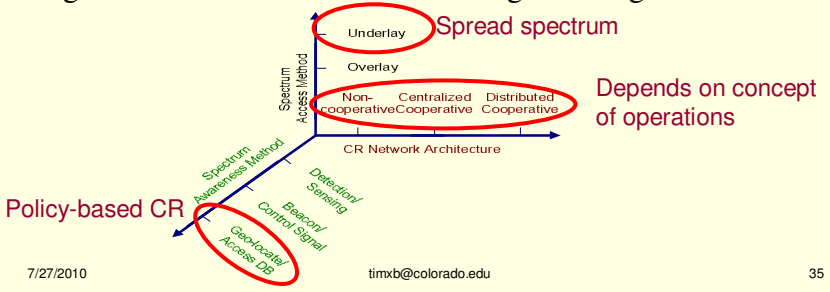
Disaster Cellular: Handset

Disaster Cellular: Base-Station

Least Vulnerable CR Configurations

Conclusion

- CRs are susceptible to attacks.
- CRs open new avenues of attack.
- A Formal Risk Analysis and Assessment Process can help guide the least vulnerable CR Design Paradigm



Are we done?

- Not quite:
  - Software defined radios
    - Malicious DSP software
  - Hardware
    - Separating CR from rest of device
    - Limits: Intermods and Spurs

(Confidentiality, Integrity, Availability)

References

- Brown, T.X, Sethi, A., "Hammer Model Threat Assessment of Cognitive Radio Denial of Service Attacks," *Proc. Of Dynamic Spectrum Access Networks,* Chicago, 2008.
- M. Barbeau, "WiMax/802.16 Threat Analysis" in *Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks,* Quebec, Canada, 2005.
- U. S. Department of Transportation, Federal Aviation Administration. (2005, Jan). System safety process steps. [Online]. Available: http://www.faa.gov/library/manuals/aviation/risk_management/media/ssprocdscrp.pdf (accessed Jun 1, 2007).